

OAK RIDGE BOARD OF EDUCATION

Monitoring: Review: Annually, in "April"	Descriptor Term: Internet Safety And Use of Digital Technology	Descriptor Code: 4.406	Issued Date: June 25, 2012
		Rescinds:	Issued:

The Oak Ridge Schools District's Internet Safety and Acceptable Use Policy is intended to prevent unauthorized access and other unlawful activities by users online, prevent unauthorized disclosure of or access to sensitive information, and to comply with the Children's Internet Protection Act (CIPA). This policy applies to all Oak Ridge Schools' students and employees, including permanent, temporary, part-time, and substitute employees, as well as volunteers, interns and contractor personnel, whose access to, or use of, Internet and/or e-mail services is funded by Oak Ridge Schools. This policy is not intended to be all-inclusive but is intended to provide reasonable guidance for the acceptable use of district network, Information Technology Resources, Internet access and e-mail. Questions about specific activities not enumerated in the policy should be directed to the user's supervisor. In compliance with the requirements of CIPA, Oak Ridge Schools has implemented a filtering system to filter or block inappropriate material.

Network Access

The following actions are not permitted (inclusive of, but not limited to :)

- A. Users will not use the district's electronic technologies to access, review, upload, download, complete, store, print, post, receive, transmit or distribute:
 - 1. Pornographic, obscene or sexually explicit material or other visual depictions;
 - 2. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful or sexually explicit language;
 - 3. Materials that use language or images that are inappropriate in the education setting or disruptive to the educational process;
 - 4. Materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment, discrimination or threatens the safety of others;
- B. Users will not use the district's electronic technologies to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.
- C. Users will not use the district's electronic technologies to engage in any illegal act or violate any local, state or federal laws.
- D. Users will not use the district's electronic technologies to vandalize damage or disable the property of another person or organization. Users will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses, engaging in "spamming" or by any other means. Users will not tamper with, modify or change the district system software, hardware or wiring or take any action to violate the district's security system. Users will not use the district's electronic technologies in such a way as to disrupt the use of the system by other users.

E. Users will not use the district's electronic technologies to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.

F. Users will not attempt to gain unauthorized access to the district's electronic technologies or any other system through the district's electronic technologies, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the staff member. Users must keep all account information and passwords private. For additional information regarding passwords please refer to the Oak Ridge Schools Password Guidelines.

G. Users will not use the district's electronic technologies to violate copyright laws or usage licensing agreements:

1. Users will not use another person's property without the person's prior approval or proper citation;
2. Users will not download, copy, or exchange pirated software;
3. Users will not plagiarize works found on the Internet or other information resources.

Web 2.0

Users accessing or using Web 2.0 products including but not limited to blogs, wikis, podcasts, Google applications and Social Networking Sites as part of their job duties or student assignments are required to keep personal information out of their postings. Students and staff will not post or give out photographs of students, their family name, password, user name, email address, home address, school name, city, country or other information that could help someone locate or contact a student in person. Speech that is inappropriate for class is not appropriate on Web 2.0 tools. Users are expected to treat others and their ideas online with respect.

Cyber Bullying

Per release of the FCC (Federal Communications Commission) and CIPA (Children's Internet Protection Act) to prohibit inappropriate online behavior which includes interaction with other individuals, students and staff shall not use cell phones, instant messaging, e-mail, chat rooms, social networking sites, or other type of digital technology to bully, threaten, discriminate, or intimidate others. If a student or staff member receives a text, e-mail, blog comment, social network post, or message via other Web 2.0 tool that makes them feel uncomfortable or is not respectful, they must report the incident to the school administrator or building designee, and must not respond to the comment. This policy includes "cyberbaiting", a term used for students deliberately provoking a teacher until they lose their composure in order to capture video that is then posted in a public forum online. Any staff member who suspects they have been targeted should immediately inform their supervisor.

Penalties for Improper Use

All users of the district's computer network, including access to the Internet, must understand that use is a privilege, not a right, and that any such use entails responsibility. Violations of acceptable use may result in disciplinary or legal action in line with existing practice regarding inappropriate conduct. When applicable, law enforcement agencies may be involved.

Student Internet Safety

Students will be instructed as to safe and responsible use of the Internet using readily available and age appropriate tools and information, as the curriculum permits. Students must abide by all laws, this

Acceptable Use Policy and all District security policies when using the District network. For additional information regarding students and internet safety please refer to the student discipline handbook.

Legal References:

- 1.TCA 39-14-602
2. TCA 10-7-512

Cross References:

Children's Internet Protection Act (CIPA)
Oak Ridge Schools Discipline Code of Conduct